SPYWOLF

Security Audit Report

Audit prepared for

PerrySwap

Completed on

March 06, 2024

KEY RESULTS

Cannot mint new tokens	Passed
Cannot pause trading (honeypot)	Not Passed
Cannot blacklist an address	Passed
Cannot raise taxes over 25%?	Passed
No proxy contract detected	Passed
Not required to enable trading	Not Passed
No hidden ownership	Passed
Cannot change the router	Passed
No cooldown feature found	Passed
Bot protection delay is lower than 5 blocks	Passed
Cannot set max tx amount below 0.05% of total supply	Passed
The contract cannot be self-destructed by owner	Passed

For a more detailed and thorough examination of the heightened risks, refer to the subsequent parts of the report.

N/A = Not applicable for this type of contract

*Only new deposits/reinvestments can be paused

OVERVIEW

This goal of this report is to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a a summarized review of the following key points:

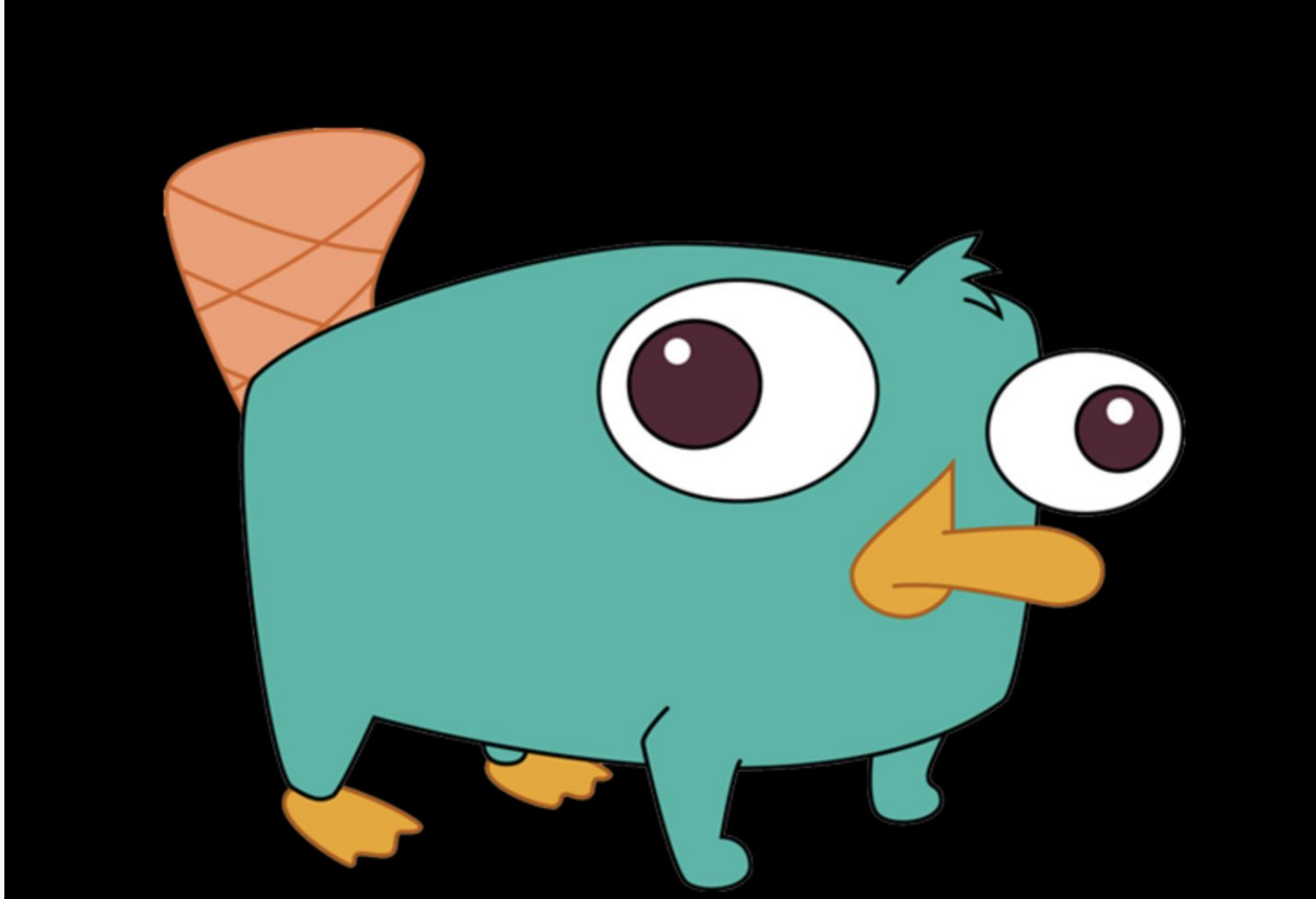
- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team’s evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

PerrySwap



PROJECT DESCRIPTION

According to their whitepaper:

PerrySwap, represented by the symbol Perry, stands at the forefront of the evolving landscape of decentralized finance (DeFi), offering a platform that redefines the way users engage with digital assets. PerrySwap is a decentralized finance (DeFi) platform offering a full suite of tools to explore and engage with the future of wealth building, overseen by the PerrySwap Decentralized Autonomous Organization (DAO).

Release Date: Presale starts in March, 2024

Category: Utility token

CONTRACT INFO

Token Name
PerrySwap

Symbol
Perry

Contract Address
0xD1f0e8be062523b764F2EB3304fE9fD8AE511377

Network
Binance Smart Chain

Language
Solidity

Deployment Date
March 06, 2024

Contract Type
Token with taxes

Total Supply
420,690,000,000,000

Status
Not launched

TAXES

Buy Tax
3%

Sell Tax
3%

*Taxes cannot be changed

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	1
Uniq Senders	1
Uniq Receivers	1
Total Amount	420690000000000 Perry
Median Transfer Amount	420690000000000 Perry
Average Transfer Amount	420690000000000 Perry
First transfer date	2024-03-06
Last transfer date	2024-03-06
Days token transferred	1

SMART CONTRACT STATS

Calls Count	1
External calls	1
Internal calls	0
Transactions count	1
Uniq Callers	1
Days contract called	1
Last transaction time	2024-03-06 05:37:52 UTC
Created	2024-03-06 05:37:52 UTC
Create TX	0x08fbb65f57bdbc5242845e93cae821d32bc788518d8399710b0fe7bf6464b7d3
Creator	0xcd6f12fd03429ffa5a2fbe6372c307962435a17e

FEATURED WALLETS

Owner address	0xcd6F12FD03429fFa5A2Fbe6372C307962435A17e
Marketing fee receiver	0xC5685f03bBcDdEb44e3D11dA6283aCE3d61528C8
LP address	0xC958163819AA6c96d436cCA635ea29BBEF25D4F5

TOP 3 UNLOCKED WALLETS

100%	Same as owner Tokens are not distributed yet
N/A	
N/A	

VULNERABILITY ANALYSIS

ID	Title	
SWC-100	Function Default Visibility	**Passed**
SWC-101	Integer Overflow and Underflow	**Passed**
SWC-102	Outdated Compiler Version	**Passed**
SWC-103	Floating Pragma	**Passed**
SWC-104	Unchecked Call Return Value	**Passed**
SWC-105	Unprotected Ether Withdrawal	**Passed**
SWC-106	Unprotected SELFDESTRUCT Instruction	**Passed**
SWC-107	Reentrancy	**Passed**
SWC-108	State Variable Default Visibility	**Passed**
SWC-109	Uninitialized Storage Pointer	**Passed**
SWC-110	Assert Violation	**Passed**
SWC-111	Use of Deprecated Solidity Functions	**Passed**
SWC-112	Delegatecall to Untrusted Callee	**Passed**
SWC-113	DoS with Failed Call	**Passed**
SWC-114	Transaction Order Dependence	**Passed**
SWC-115	Authorization through tx.origin	**Passed**
SWC-116	Block values as a proxy for time	**Passed**
SWC-117	Signature Malleability	**Passed**
SWC-118	Incorrect Constructor Name	**Passed**

VULNERABILITY ANALYSIS

ID	Title	
SWC-119	Shadowing State Variables	Passed
SWC-120	Weak Sources of Randomness from Chain Attributes	Passed
SWC-121	Missing Protection against Signature Replay Attacks	Passed
SWC-122	Lack of Proper Signature Verification	Passed
SWC-123	Requirement Violation	Passed
SWC-124	Write to Arbitrary Storage Location	Passed
SWC-125	Incorrect Inheritance Order	Passed
SWC-126	Insufficient Gas Griefing	Passed
SWC-127	Arbitrary Jump with Function Type Variable	Passed
SWC-128	DoS With Block Gas Limit	Passed
SWC-129	Typographical Error	Passed
SWC-130	Right-To-Left-Override control character (U+202E)	Passed
SWC-131	Presence of unused variables	Passed
SWC-132	Unexpected Ether balance	Passed
SWC-133	Hash Collisions With Multiple Variable Length Arguments	Passed
SWC-134	Message call with hardcoded gas amount	Passed
SWC-135	Code With No Effects	Passed
SWC-136	Unencrypted Private Data On-Chain	Passed

VULNERABILITY ANALYSIS

NO ERRORS FOUND

MANUAL
CODE REVIEW

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time.

We categorize these vulnerabilities by 4 different threat levels.

THREAT LEVELS

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance, functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ High Risk

tradingEnabled is currently false, allowing vetted addresses to potentially sell their presale tokens before opening trade for the investors.

Note: This only applies if launching on a launchpad platform like Pinksale.

```
function EnableTrading() external onlyOwner {
    require(!tradingEnabled, "Cannot re-enable trading.");
    tradingEnabled = true;
    swapEnabled = true;
    genesis_block = block.number;
}
```

- Recommendation:
  - Once presale is finished and trading is not enabled, investors cannot sell their token holdings on token launch. Trading should be enabled before presale finish and token launch on DEX.

FOUND THREATS

⚠ High Risk

Owner can change marketing/dev/ops wallets.
If any of the above is set to contract address that cannot receive BNB and/or contract balances are zero, contract will halt on sell.

```
function updateMarketingWallet(address newWallet) external onlyOwner {
    require(newWallet != address(0),"Fee Address cannot be dead address.");
    marketingWallet = newWallet;
}

function updateDevWallet(address newWallet) external onlyOwner {
    require(newWallet != address(0),"Fee Address cannot be dead address.");
    devWallet = newWallet;
}

function updateOpsWallet(address newWallet) external onlyOwner {
    require(newWallet != address(0),"Fee Address cannot be dead address.");
    opsWallet = newWallet;
}

function sendValue(address payable recipient, uint256 amount) internal {
    require(address(this).balance >= amount, "Address: Insufficient balance.");

    (bool success, ) = recipient.call{ value: amount }("");
    require(success, "Address: Unable to send value, recipient may have reverted.");
}

function _tokenTransfer(
    address sender, address recipient, uint256 tAmount,
    bool takeFee, bool isSell
) private {
.....................
uint256 marketingAmt = unitBalance * 2 * temp.marketing;
    if (marketingAmt > 0) {
        payable(marketingWallet).sendValue(marketingAmt);
    }

    uint256 devAmt = unitBalance * 2 * temp.dev;
    if (devAmt > 0) {
        payable(devWallet).sendValue(devAmt);
    }

    uint256 opsAmt = unitBalance * 2 * temp.ops;
    if (opsAmt > 0) {
        payable(opsWallet).sendValue(opsAmt);
    }
}
```

- Recommendation:
  - Remove the require statements in sendValue() function

FOUND THREATS

⚠ High Risk

Owner can change contract's auto swap settings.
If swapTokensAtAmount is set to zero or very low number, contract will halt on sell.

```
function updateSwapTokensAtAmount(uint256 amount) external onlyOwner {
    require(amount <= 42e14, "Can't set swap threshold amount higher than 1% of tokens.");
    swapTokensAtAmount = amount * 10**_decimals;
}

function _transfer(
    address from,
    address to,
    uint256 amount
) private {
.....................
bool canSwap = balanceOf(address(this)) >= swapTokensAtAmount;
if (
    !swapping &&
    swapEnabled &&
    canSwap &&
    from != pair &&
    !_isExcludedFromFee[from] &&
    !_isExcludedFromFee[to]
) {
    if (to == pair) swapAndLiquify(swapTokensAtAmount, sellTaxes);
    else swapAndLiquify(swapTokensAtAmount, taxes);
}
.....................
}
```

- Recommendation:
  - Ensure that swapTokensAtAmount's value is always above 1 token (consider decimals)

FOUND THREATS

Informational

Owner can set time to apply launch tax up to 5 blocks after initial trading start.
Launch tax is 99%, up to 5 blocks after initial trading start.

```
function updatedeadline(uint256 _deadline) external onlyOwner {
    require(!tradingEnabled, "Can't change when trading has started.");
    require(_deadline < 5,"Deadline should be less than 5 Blocks.");
    deadline = _deadline;
}
```

Owner can exclude address from reflections rewards.

```
function excludeFromReward(address account) public onlyOwner {
    require(!_isExcluded[account], "Account is already excluded.");
    if (_rOwned[account] > 0) {
        _tOwned[account] = tokenFromReflection(_rOwned[account]);
    }
    _isExcluded[account] = true;
    _excluded.push(account);
}
```

FOUND THREATS

Informational

Owner can withdraw any tokens from the contract except of native Perry token.
When this function is present, in cases tokens/bnb are sent into the contract by mistake or purposefully, contract's owner can retrieve them.

```
function rescueBNB(uint256 weiAmount) external onlyOwner {
    require(address(this).balance >= weiAmount, "Insufficient BNB balance.");
    payable(msg.sender).transfer(weiAmount);
}

function rescueAnyBEP20Tokens(address _tokenAddr,address _to, uint256 _amount) public onlyOwner {
    require(_tokenAddr != address(this), "Owner can't claim contract's balance of its own tokens.");
    IBEP20(_tokenAddr).transfer(_to, _amount);
}
```

Owner can exclude address from fees.
When address is excluded from fees, the user will receive the whole amount of the bought, sold and/or transferred tokens.

```
function excludeFromFee(address account) public onlyOwner {
    _isExcludedFromFee[account] = true;
}

function bulkExcludeFee(address[] memory accounts, bool state) external onlyOwner {
    for (uint256 i = 0; i < accounts.length; i++) {
        _isExcludedFromFee[accounts[i]] = state;
    }
}
```

There is no information about the initial tokens distribution based on the project's whitepaper and/or website.

TOKENOMICS

WEBSITE

Website URL
https://perry.finance/

Domain Registry
https://www.hostinger.com

Domain Expiration
2025-03-05

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

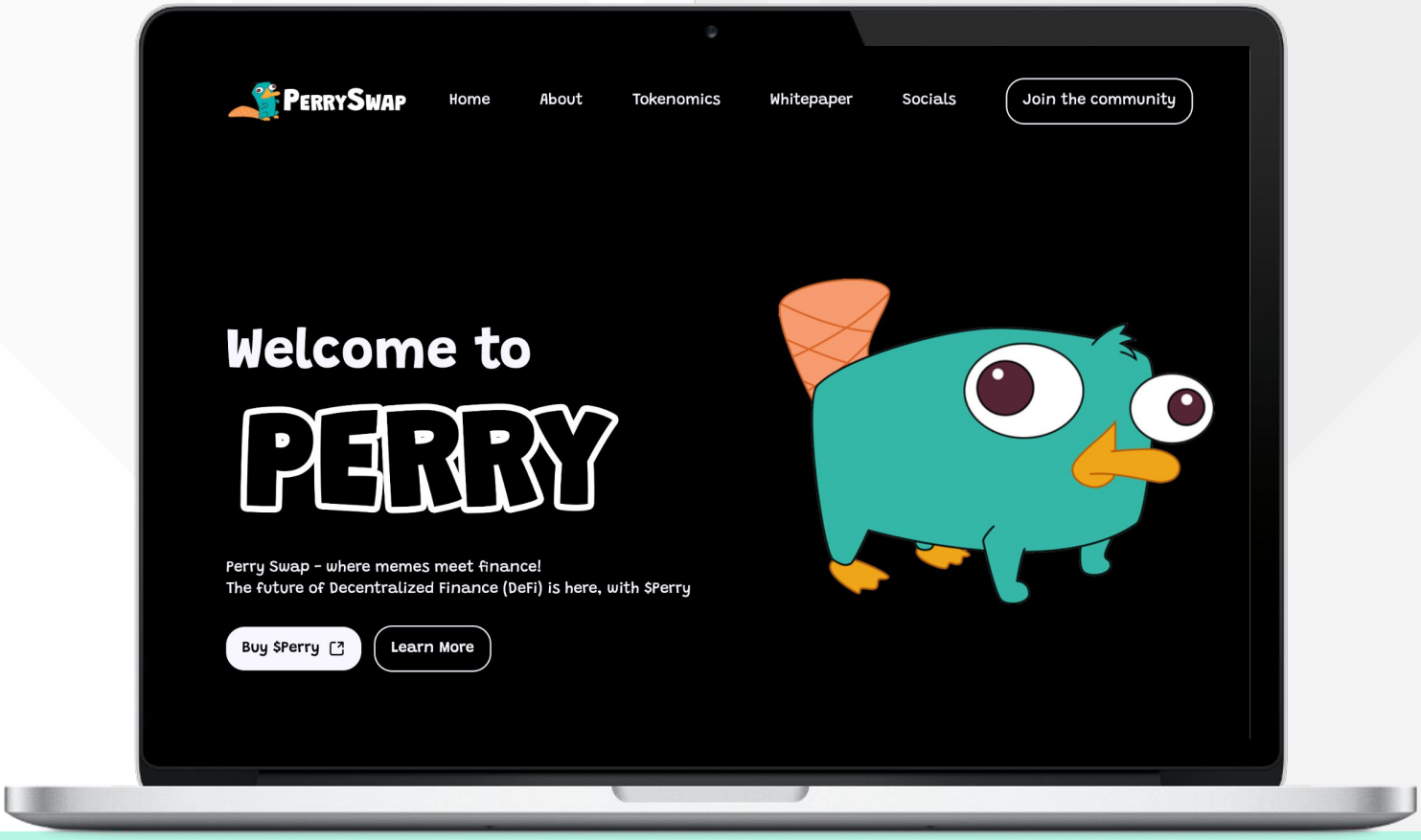
Design
Single page design with appropriate color scheme and graphics.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.

Whitepaper
Well written but a bit short

Roadmap
No

Mobile-friendly?
Yes



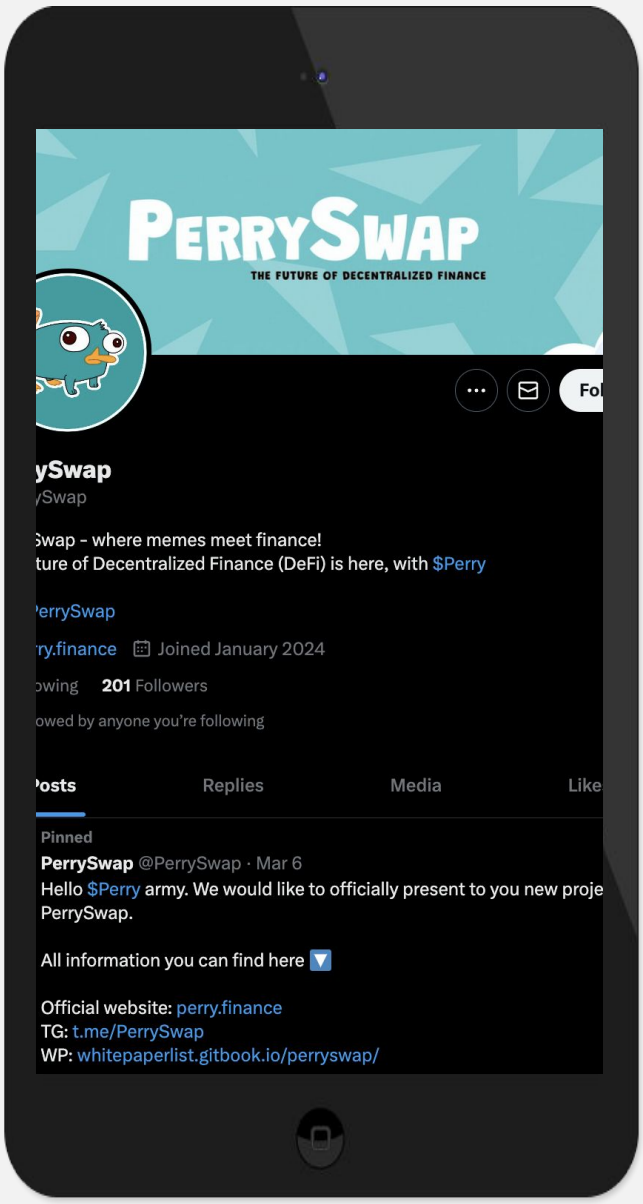
perry.finance

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project's social media pages are active



Twitter's X

@PerrySwap

- 202 followers
- 3 total posts
- New account

Discord

- Not available

Telegram

@PerrySwap

- 42 members
- Active users
- Active mods

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 700 SUCCESSFUL CLIENTS**
- **MORE THAN 1000 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.